

DERWENT-ACC-NO: 1999-463857

DERWENT-WEEK: 199939

COPYRIGHT 1999 DERWENT INFORMATION LTD

TITLE: Booting file production in client server system -
produces booting file based on information acquired by
Java agent that is transmitted along with DHCP packet
from DHCP server to client

PATENT-ASSIGNEE: TOSHIBA KK[TOKE]

PRIORITY-DATA: 1997JP-0366814 (December 26, 1997)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
JP 11195000 A	July 21, 1999	N/A	007	G06F 015/00

APPLICATION-DATA:

PUB-NO	APPL-DESCRIPTOR	APPL-NO	APPL-DATE
JP 11195000A	N/A	1997JP-0366814	December 26, 1997

INT-CL (IPC): G06F009/06, G06F013/00 , G06F015/00

ABSTRACTED-PUB-NO: JP 11195000A

BASIC-ABSTRACT:

NOVELTY - When the client (15) is switched ON, a dynamic host configuration protocol (DHCP) packet (16) along with Java agent (17) is transmitted from DHCP server (13) to the client. The Java agent acquires information for producing booting file by communicating with other servers. Booting of client is performed by the booting file produced by Java agent. DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for booting procedure in client server system.

USE - In client server system.

ADVANTAGE - Booting file can be determined flexibly. DESCRIPTION OF DRAWING(S)
- The figure shows the block diagram of client server system. (13) DHCP server; (15) Client; (16) DHCP packet; (17) Java agent.

CHOSEN-DRAWING: Dwg.1/3

TITLE-TERMS: FILE PRODUCE CLIENT SERVE SYSTEM PRODUCE FILE BASED
INFORMATION

ACQUIRE AGENT TRANSMIT PACKET SERVE CLIENT

DERWENT-CLASS: T01

EPI-CODES: T01-F06; T01-H; T01-J;

SECONDARY-ACC-NO:

Non-CPI Secondary Accession Numbers: N1999-347526

【特許請求の範囲】

【請求項1】 クライアント計算機と、このクライアント計算機に各種のサービスを提供するサーバ計算機と、このサーバ計算機と上記クライアント計算機を接続するネットワーク等の通信網とからなる計算機システムに於いて、

上記サーバ計算機は、

上記クライアント計算機にIPアドレスを割り当てるアドレス割り当て手段と、

上記クライアント計算機のユーザを認証するユーザ認証手段と、

上記クライアント計算機のユーザが利用するユーザ固有の情報を記憶するユーザ情報記憶手段と、

上記クライアント計算機を立ち上げる際必要となる起動情報を作成する起動情報作成手段とを有し、

上記クライアント計算機は、

上記ユーザのユーザ認証情報と上記クライアント計算機に関する情報と上記サーバ計算機に上記起動情報を請求する情報とを持つ起動情報請求パケットにエージェントを付加するエージェント付加手段を有して、

上記クライアント計算機を立ち上げる際、上記クライアント計算機は上記起動情報請求パケットを上記サーバ計算機に送信し、

上記アドレス割り当て手段は上記起動情報請求パケットから上記クライアント計算機の情報を読み出して上記クライアント計算機にIPアドレスを割り当て付加されているエージェントを上記起動情報作成手段に転送し、

この転送されたエージェントは自分自身を上記ユーザ認証手段と上記ユーザ情報記憶手段へコピーし、

上記ユーザ認証手段にコピーされたエージェントは、上記ユーザのユーザ認証情報と上記クライアント計算機に関する情報に基づき上記起動情報作成手段と上記クライアント計算機へ通信して上記ユーザと上記クライアント計算機の認証処理を行い、

上記ユーザ情報記憶手段へコピーされたエージェントは、上記ユーザ認証手段のエージェントと上記クライアント計算機へ通信して記憶されているユーザ固有の情報に関する情報を作成し、

上記起動情報作成手段に転送されたエージェントは、上記ユーザ認証手段のエージェントから認証処理に関する情報の通知を受け、上記ユーザ情報記憶手段のエージェントとからはユーザ固有の情報に関する情報の通知を受け、これらの情報に基づいて起動情報を作成することを特徴とする計算機システム。

【請求項2】 クライアント計算機と、このクライアント計算機に各種のサービスを提供する複数のサーバ計算機と、これら複数のサーバ計算機と上記クライアント計算機を接続するネットワーク等の通信網とからなる計算機システムに於いて、

上記複数のサーバ計算機には、

上記クライアント計算機にIPアドレスを割り当てるアドレス割り当てサーバ計算機と、

上記クライアント計算機のユーザを認証するユーザ認証サーバ計算機と、上記クライアント計算機のユーザが利用するユーザ固有の情報を記憶するユーザ情報記憶サーバ計算機と、

上記クライアント計算機を立ち上げる際必要となる起動情報を作成する起動情報作成サーバ計算機とを設け、

上記クライアント計算機には、

10 上記ユーザのユーザ認証情報と上記クライアント計算機に関する情報と上記起動情報作成サーバ計算機に上記起動情報を請求する情報とを持つ起動情報請求パケットにエージェントを付加するエージェント付加手段を設けて、

上記クライアント計算機を立ち上げる際、上記クライアント計算機は上記起動情報請求パケットを上記アドレス割り当てサーバ計算機に送信し、

20 上記アドレス割り当てサーバ計算機は上記起動情報請求パケットから上記クライアント計算機の情報を読み出して上記クライアント計算機にIPアドレスを割り当て付加されているエージェントを上記起動情報作成サーバ計算機に転送し、

この転送されたエージェントは、当該エージェント自体を上記ユーザ認証サーバ計算機と上記ユーザ情報記憶サーバ計算機へコピーし、

上記ユーザ認証サーバ計算機にコピーされたエージェントは、上記ユーザのユーザ認証情報と上記クライアント計算機に関する情報に基づき上記起動情報作成サーバ計算機と上記クライアント計算機へ通信して上記ユーザと

30 上記クライアント計算機の認証処理を行い、上記ユーザ情報記憶サーバ計算機へコピーされたエージェントは、上記ユーザ認証サーバ計算機のエージェントと上記クライアント計算機へ通信して記憶されているユーザ固有の情報に関する情報を作成し、

上記起動情報作成サーバ計算機に転送されたエージェントは、上記ユーザ認証サーバ計算機のエージェントから認証処理に関する情報の通知を受け、上記ユーザ情報記憶サーバ計算機のエージェントとからはユーザ固有の情報に関する情報の通知を受け、これらの情報に基づいて

40 起動情報を作成することを特徴とする計算機システム。
【請求項3】 上記エージェントは、上記クライアント計算機を立ち上げる際に必要な情報を得た後、自らを削除することを特徴とする請求項1又は2記載の計算機システム。

【請求項4】 クライアント計算機と、このクライアント計算機に各種のサービスを提供するサーバ計算機と、このサーバ計算機と上記クライアント計算機を接続するネットワーク等の通信網とからなる計算機システムのクライアント計算機の起動制御方法に於いて、

50 上記サーバ計算機は、

上記クライアント計算機にIPアドレスを割り当てるアドレス割り当て手段と、

上記クライアント計算機のユーザを認証するユーザ認証手段と、

上記クライアント計算機のユーザが利用するユーザ固有の情報を記憶するユーザ情報記憶手段と、

上記クライアント計算機を立ち上げる際、必要となる起動情報を作成する起動情報作成手段とを設け、

上記クライアント計算機を立ち上げる際、上記クライアント計算機は上記ユーザのユーザ認証情報と上記クライアント計算機に関する情報と上記サーバ計算機に上記起動情報を請求する情報とを持つ起動情報請求パケットにエージェントを付加して上記サーバ計算機に送信し、

上記アドレス割り当て手段は上記起動情報請求パケットから上記クライアント計算機の情報を読み別して上記クライアント計算機にIPアドレスを割り当て付加されているエージェントを上記起動情報作成手段に転送し、

この転送されたエージェントは、自分自身を上記ユーザ認証手段と上記ユーザ情報記憶手段へコピーし、

上記ユーザ認証手段にコピーされたエージェントは、上記ユーザのユーザ認証情報と上記クライアント計算機に関する情報に基づき上記起動情報作成手段と上記クライアント計算機へ通信して上記ユーザと上記クライアント計算機の認証処理を行い、

上記ユーザ情報記憶手段へコピーされたエージェントは、上記ユーザ認証手段のエージェントと上記クライアント計算機へ通信して記憶されているユーザ固有の情報に関する情報を作成し、

上記起動情報作成手段に転送されたエージェントは、上記ユーザ認証手段のエージェントから認証処理に関する情報の通知を受け、上記ユーザ情報記憶手段のエージェントとからはユーザ固有の情報に関する情報の通知を受け、これらの情報に基づいて起動情報を作成することを特徴とするクライアント計算機の起動制御方法。

【請求項5】 クライアント計算機と、このクライアント計算機に各種のサービスを提供する複数のサーバ計算機と、これら複数のサーバ計算機と上記クライアント計算機を接続するネットワーク等の通信網とからなる計算機システムのクライアント計算機起動制御方法に於いて、

上記複数のサーバ計算機には、

上記クライアント計算機にIPアドレスを割り当てるアドレス割り当てサーバ計算機と、

上記クライアント計算機のユーザを認証するユーザ認証サーバ計算機と、

上記クライアント計算機のユーザが利用するユーザ固有の情報を記憶するユーザ情報記憶サーバ計算機と、

上記クライアント計算機を立ち上げる際、必要となる起動情報を作成する起動情報作成サーバ計算機とを設け、

上記クライアント計算機を立ち上げる際、上記クライ

アント計算機は上記ユーザのユーザ認証情報と上記クライアント計算機に関する情報と上記起動情報作成サーバ計算機に上記起動情報を請求する情報とを持つ起動情報請求パケットにエージェントを付加して上記アドレス割り当てサーバ計算機に送信し、

上記アドレス割り当てサーバ計算機は、上記起動情報請求パケットから上記クライアント計算機の情報を読み別して上記クライアント計算機にIPアドレスを割り当て付加されているエージェントを上記起動情報作成サーバ計算機に転送し、この転送されたエージェントは、自分自身を上記ユーザ認証サーバ計算機と上記ユーザ情報記憶サーバ計算機へコピーし、

上記ユーザ認証サーバ計算機にコピーされたエージェントは、上記ユーザのユーザ認証情報と上記クライアント計算機に関する情報に基づき上記起動情報作成サーバ計算機と上記クライアント計算機へ通信して上記ユーザと上記クライアント計算機の認証処理を行い、

上記ユーザ情報記憶サーバ計算機へコピーされたエージェントは、上記ユーザ認証サーバ計算機のエージェントと上記クライアント計算機へ通信して記憶されているユーザ固有の情報に関する情報を作成し、

上記起動情報作成サーバ計算機に転送されたエージェントは、上記ユーザ認証サーバ計算機のエージェントから認証処理に関する情報の通知を受け、上記ユーザ情報記憶サーバ計算機のエージェントとからはユーザ固有の情報に関する情報の通知を受け、これらの情報に基づいて起動情報を作成することを特徴とするクライアント計算機の起動制御方法。

【請求項6】 上記エージェントは、上記クライアント計算機を立ち上げる際に必要な情報を得た後、自らを削除することを特徴とする請求項4又は5記載のクライアント計算機の起動制御方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、クライアント計算機と、このクライアント計算機からの要求に応じて各種のサービスを提供するサーバ計算機と、このサーバ計算機と上記クライアント計算機を接続するネットワーク等の通信網とからなる計算機システムに於いて、携帯端末等のコンピュータである上記クライアント計算機を立ち上げる際の起動制御方法に係る計算機システム、及び計算機システムのクライアント計算機の起動制御方法に関する。

【0002】

【従来の技術】従来、クライアントサーバシステムにおける携帯端末等のクライアント計算機（クライアント）のブート（立ち上げ）方式として、ブート情報請求のためにBOOTPやDHCP（Dynamic Host Configuration Protocol）のプロトコルを利用したものが広く用いられている。このブート方式では、ブートサーバがクラ

クライアントに転送するブートファイルが、以下のように決定されていた。

【0003】・クライアント側で固定

・サーバ(サーバ計算機)側で固定

・サーバ側で、クライアントのMACアドレス等で決定

【0004】

【発明が解決しようとする課題】上述したように従来のブート方式では、ブートサーバがクライアントに転送するブートファイルが上記のように決定されていた。これらの方式では、クライアントのMACアドレスが予め分かっているなどの前提があるか、またはファイル名が固定されている等、柔軟性や安全性に欠けることがあった。このため、サーバに対して多くのクライアントが接続される場合の、クライアントのブートには不向きであった。

【0005】前述のように、BOOTPやDHCPプロトコルを利用したブート方式は、柔軟性や安全性に欠ける問題点があった。

【0006】そこで、本発明は上記事情を考慮して成されたもので、上記不具合を解消し、携帯端末等のコンピュータであるクライアント計算機(以下クライアント)と、有線や無線のLAN(Local area network)等のネットワーク等からなる通信網と、この通信網により接続されているクライアントからの要求に応じて各種のサービスを提供するサーバ計算機(以下サーバ)とからなる計算機システムにおいて、クライアントがブート時に使用するDHCPパケットにJavaエージェントを付加し、このJavaエージェントが各サーバに自分自身を転送、コピーし、そのエージェント同士が通信を行うことによりブートファイルを決定し、また認証サーバにアクセス可能として、これにより信頼性の高い、かつ柔軟なブート手段を有する計算機システム、及び計算機システムのクライアント計算機の起動制御方法を提供することを目的とする。

【0007】

【課題を解決するための手段】本発明は上記目的を達成するため、本発明の計算機システムは、クライアント計算機とこのクライアント計算機に各種のサービスを提供するサーバ計算機とこのサーバ計算機と上記クライアント計算機を接続するネットワーク等の通信網からなる計算機システムにおいて、上記サーバ計算機は、上記クライアント計算機にIPアドレスを割り当てるアドレス割り当て手段と、上記クライアント計算機のユーザを認証するユーザ認証手段と、上記クライアント計算機のユーザが利用するユーザ固有の情報を記憶するユーザ情報記憶手段と、上記クライアント計算機を立ち上げる際必要となる起動情報を作成する起動情報作成手段とを設け、上記クライアント計算機は、上記ユーザのユーザ認証情報と上記クライアント計算機に関する情報と上記サーバ計算機に上記起動情報を請求する情報とを持つ起動情報

請求パケットにエージェントを付加するエージェント付加手段を設け、上記クライアント計算機を立ち上げる際上記クライアント計算機は、上記起動情報請求パケットを上記サーバ計算機に送信し、上記アドレス割り当て手段は上記起動情報請求パケットから上記クライアント計算機の情報を読み取り上記クライアント計算機にIPアドレスを割り当て付加されているエージェントを上記起動情報作成手段に転送し、この転送されたエージェントは自分自身を上記ユーザ認証手段と上記ユーザ情報記憶手段へコピーし、上記ユーザ認証手段にコピーされたエージェントは上記ユーザのユーザ認証情報と上記クライアント計算機に関する情報に基づき上記起動情報作成手段と上記クライアント計算機へ通信して上記ユーザと上記クライアント計算機の認証処理を行い、上記ユーザ情報記憶手段へコピーされたエージェントは上記ユーザ認証手段のエージェントと上記クライアント計算機へ通信して記憶されているユーザ固有の情報に関する情報を作成し、上記起動情報作成手段に転送されたエージェントは上記ユーザ認証手段のエージェントから認証処理に関する情報の通知を受け、上記ユーザ情報記憶手段のエージェントとからはユーザ固有の情報に関する情報の通知を受け、これらの情報に基づいて起動情報を作成することを特徴とする。

【0008】上記構成によれば、クライアント計算機を立ち上げる際、立ち上げるに必要な起動ファイルをサーバ計算機へ請求する時、エージェントを付加して送信し、このエージェントがサーバ計算機の各手段に自分自身を転送、コピーして、互いに通信しあい必要な情報を得ることによって、起動ファイルを決定する。これにより信頼性の高い、かつ柔軟なブート手段を提供できる。

【0009】また、上記サーバ計算機の各手段は各々別のサーバ計算機に設けても良いし、上記エージェントはクライアント計算機の立ち上げに必要な情報を全て獲得し起動処理が終了したら、自分自身を削除するようにしても良い。

【0010】

【発明の実施の形態】以下、図面を参照して本発明の一実施の形態を説明する。

【0011】図1は、本発明の実施形態に係わるブート方法を採用したクライアント-サーバシステムの一般的な構成を示した図である。図1では、クライアント15は、ネットワーク20に存在し、DHCPサーバ13、ブートサーバ12、ユーザのホームサーバ11は、ネットワーク19に存在し、認証サーバ10はネットワーク18に存在する場合を例にとって説明する。

【0012】まず、図1の各構成について説明する。

【0013】クライアント15は、パーソナルコンピュータや携帯端末等のコンピュータであり、ネットワーク20を通じて各サーバにアクセスし各種サービス等の要求等を行う。

【0014】認証サーバ10は、ネットワークにアクセスするクライアント15が、各サーバからの各種サービスを受けることを予め許可されたクライアントかどうかの認証を行う。

【0015】ホームディレクトリサーバ11は、クライアント15のユーザのホームサーバである。ユーザが利用するユーザ固有の情報等が管理されている。

【0016】ブートサーバ12は、クライアント15を立ち上げる場合に必要となるファイルであるブートファイルをクライアント15に転送する。

【0017】DHCPサーバ13は、クライアント15が立ち上げ時に送信するDHCPパケットを受信してクライアント情報を識別し、IPアドレスを割り当て、ブートサーバ12へ転送する。

【0018】DHCPリレーサーバ14は、クライアント15が立ち上げ時に送信するDHCPパケットを受信してDHCPサーバ14へ転送するための中継サーバである。

【0019】DHCPパケット16は、クライアント15が立ち上げ時に送信する送信パケットである。図2により、このDHCPパケット16に含まれる情報を説明する。

【0020】IP21は、クライアント-サーバ間の通信に必要なIP (Internet Protocol) の情報である。UDP22は、クライアント-サーバ間の通信に必要なUDP (User Datagram Protocol) の情報である。DHCPパケット23は、クライアント15が立ち上げ時に必要とするブートファイルを請求するための情報である。

【0021】Javaエージェント17は、Java (米Sun Microsystem 社のオブジェクト指向言語) で作成されたプログラムをサーバからダウンロードし実行するなどの制御をする。また、Javaエージェント17は、DHCPサーバ13に送信された後、ブートサーバ12に転送される。その後、自分自身をコピーして認証サーバ10、ホームサーバ11へ送信し、各サーバ間の通信を行い、ブートファイルを決定する。

【0022】クライアント情報25は、クライアントのアドレス等のクライアント15に関する情報である。

【0023】ユーザ情報26は、ユーザを識別するためにネットワーク上で使用するユーザ名等の情報である。

【0024】認証情報27は、認証サーバ10がネットワーク18に入るユーザを認証するためのパスワード等のユーザ認証情報である。

【0025】次に、クライアント15を立ち上げる際にJavaエージェント17によりブートファイルを決定するまでの処理動作を、図3のフローチャートを参照して説明する。

【0026】クライアント15は、立ち上げ時(ステップA1)、ブートファイルを請求するためのDHCPパ

ケット16にJavaエージェント17を付加してDHCPサーバ13へ送信する(ステップA2)。

【0027】DHCPパケット16は、DHCPリレーサーバ14の中継によりDHCPサーバ13へ送信される。

【0028】DHCPサーバ13は、DHCPパケット16からJavaエージェント17を認識して、その後、クライアント情報25を識別し、Javaエージェント17をブートサーバ12へ転送する(ステップA3)。

【0029】ブートサーバ12に転送されたJavaエージェント17は、そこで実行され、認証サーバ10、ホームサーバ11の各サーバに自分自身をコピーする(ステップA4)。

【0030】Javaエージェント17は、各サーバで処理を実行する(ステップA5)。

【0031】ここで各サーバでの処理を説明する。

【0032】認証サーバ10に送られたJavaエージェント17は、ブートサーバ12、クライアント15と通信を行い、クライアントやユーザを認証する。また、ホームサーバ11に送られたJavaエージェント17は、そこで実行され、認証サーバ10やクライアント15と通信を行い、ユーザのホームディレクトリの情報を提供する。

【0033】これらのサーバが提供する情報はブートサーバ12に集められ(ステップA6)、ブートサーバ12のJavaエージェント17はブートサーバプロセスと情報交換してブートファイルを決定し(ステップA7)、ブートファイルをクライアント15に送信する(ステップA8)。

【0034】クライアント15はこのブートファイルを利用してシステムを起動する(ステップA9)。このブートファイルが今度は各サーバのJavaエージェント17と通信を行い、ユーザ情報や認証情報を獲得する(ステップA10)。

【0035】全ての情報を得た後、これらのJavaエージェント17は自らを削除する。これで、ブートファイル決定処理は終了する。

【0036】上述したように本実施形態によれば、携帯端末等のコンピュータであるクライアント計算機(以下クライアント)と、有線や無線のLAN (Local area network) 等のネットワーク等からなる通信網と、この通信網により接続されているクライアントからの要求に応じて各種のサービスを提供するサーバ計算機(以下サーバ)とからなる計算機システムにあって、クライアントがブート時に使用するDHCPパケットにJavaエージェントを付加し、このJavaエージェントが各サーバに自分自身を転送/コピーし、そのエージェント同士が通信を行うことによりブートファイルを決定し、また認証サーバにアクセス可能とした。これにより信頼性

が高く、かつ柔軟なブート手段を有する計算機システム、及び計算機システムのクライアント計算機の起動制御方法の提供を実現できる。

【0037】なお、上記実施形態では、認証やブート等の各機能を各々サーバ別の計算機で行っているが、一つのサーバ計算機で行っても良いことは勿論である。

【0038】

【発明の効果】以上詳記したように本発明によれば、クライアントからサーバへのブート請求 packets にエージェントを付加し、このエージェントが自分自身を認証サーバ、ブートサーバ等の各サーバへコピーし、コピーされたエージェント同士が互いに通信を行い必要な情報を得ることにより、ブートファイルを柔軟に決定できることができ、かつ安全性の高いブートの実現を容易にする。

【図面の簡単な説明】

【図1】本発明の一実施の形態に係る計算機システムの構成を示すブロック図。

【図2】同実施の形態に係る DHCP パケットの持つ情報を示す図。

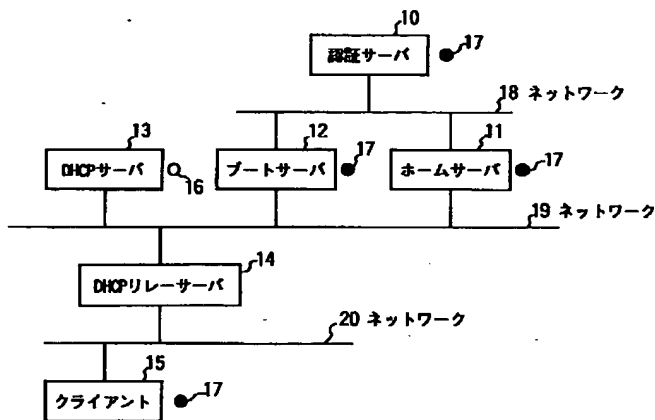
20

【図3】同実施の形態に係るクライアント立ち上げ時のブートファイル決定までの処理動作を示すフローチャート。

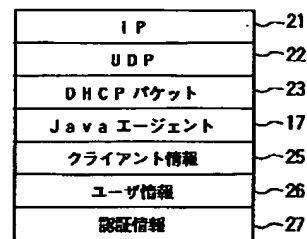
【符号の説明】

- 10…認証サーバ
- 11…ホームサーバ
- 12…ブートサーバ
- 13…DHCPサーバ
- 14…DHCPリレーサーバ
- 15…クライアント
- 16…DHCPパケット
- 17…Javaエージェント
- 18, 19, 20…ネットワーク
- 21…IP
- 22…UDP
- 23…DHCPパケット
- 25…クライアント情報
- 26…ユーザ情報
- 27…認証情報

【図1】



【図2】



【図3】

